TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire	**POUR SUITE A DONNER** voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale No. PCT/FR 03/03877	Date du dépôt international *(jour/mois/année)* 23.12.2003	Date de priorité *(jour/mois/année)* 24.12.2002
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB G06F1/00		
Déposant ENIGMA SYSTEMS SARL		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 6 feuilles, y compris la présente feuille de couverture.

   ☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent 4 feuilles.

3. Le présent rapport contient des indications et les pages correspondantes relatives aux points suivants :

I	☒	Base de l'opinion
II	☐	Priorité
III	☐	Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
IV	☐	Absence d'unité de l'invention
V	☒	Déclaration motivée selon la règle 66.2(a)(ii) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
VI	☐	Certains documents cités
VII	☐	Irrégularités dans la demande internationale
VIII	☐	Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
26.07.2004	04.03.2005
Nom et adresse postale de l'adminstration chargée de l'examen préliminaire international Office européen des brevets - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tél. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Fonctionnaire autorisé Segura, G N° de téléphone +31 70 340-4874

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR 03/03877

I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale *(les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées, dans le présent rapport, comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17))* :

Description, Pages

1-8 telles qu'initialement déposées

Revendications, No.

1-23 reçue(s) le 10.12.2004 avec lettre du 03.12.2004

Dessins, Feuilles

1/2-2/2 telles qu'initialement déposées

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

   Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: ,qui est:

   ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).

   ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).

   ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés**divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

   ☐ contenu dans la demande internationale, sous forme écrite.

   ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.

   ☐ remis ultérieurement à l'administration, sous forme écrite.

   ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listages des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

   ☐ de la description, pages :

   ☐ des revendications, nos :

   ☐ des dessins, feuilles :

5. ☒ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

   (Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport.)

   voir feuille séparée

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui:	Revendications	1-21
	Non:	Revendications	
Activité inventive	Oui:	Revendications	
	Non:	Revendications	1-21
Possibilité d'application industrielle	Oui:	Revendications	1-21
	Non:	Revendications	

2. Citations et explications

   voir feuille séparée

Concernant le point I
Base de l'opinion

1. Les revendications 22 et 23 introduites avec la lettre du 3.12.2004 conduisent à étendre l'objet de la demande au-delà du contenu de la demande telle qu'elle a été déposée. Elles vont par conséquent à l'encontre des dispositions de l'article 34(2) b) PCT. Les raisons sont les suivantes:

   Le procédé de la revendication 22 décrit deux flots de données, un flot insérant le certificat exécutable et un autre flot comprenant des données nécessaires au bon fonctionnement de l'application logicielle. Pourtant dans la déscription (page 7, lignes 6-15) il n'existe qu'un flot de données contenant les instructions de contrôle (certificat exécutable) programmées pour déchiffrer une partie **du flot** de données que l'application à vérifier doit traiter.

   Le même argument s'applique à la revendication 23.

Concernant le point V
Déclaration motivée quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Il est fait référence aux documents suivants:

   D1: US-B-6 308 2701 (GUTHERY SCOTT B) 23 octobre 2001 (2001-10-23)
   D2: WO 99/35582 A (LUI CHEW WAH) 15 juillet 1999 (1999-07-15)
   D3: US-A-6 006 328 (DRAKE CHRISTOPHER NATHAN) 21 décembre 1999 (1999-12-21)

2. La présente demande ne remplit pas les conditions énoncées dans l'article 33(1) PCT, l'objet de la revendication 1 et 13 n'impliquant pas une activité inventive telle que définie par l'article 33(3) PCT, pour les suivantes raisons:

2.1 Le document D1, qui est considéré comme étant l'état de la technique le plus proche de l'objet de la revendication 1, décrit (les références entre parenthèses s'appliquent à ce document) : un procédé de vérification de l'intégrité d'une application logicielle exécutable dans un terminal hôte comprenant les étapes suivantes: sur le terminal hôte, exécuter l'application logicielle à vérifier et exécuter une suite d'instructions de contrôle, formant certificat exécutable par le dit terminal hôte au cours de l'exécution de l'application logicielle à vérifier (colonne 4, ligne 54 - colonne 5, ligne 3; figure 5), dans le contexte mémoire de l'application logicielle (colonne 4, ligne 54 - colonne 5, ligne 3); comparer le résultat ainsi obtenu par l'exécution des instructions de contrôle avec le résultat attendu d'une application logicielle authentique (colonne 4, lignes 63-65) et; en cas de "comparaison positive", continuer le cours de l'exécution de l'application logicielle à vérifier (colonne 4, ligne 66 - colonne 5, ligne 3).

Il est à noter qu'en D1 le certificat éxecutable est formé par les instructions de l'application à vérifier qui interagissent avec une carte à puce et par les instructions réalisées par la carte à puce. Donc, une partie du certificat éxecutable **est éxecuté dans le contexte mémoire de l'application logicielle**. Il faut aussi souligner que le certificat de D1 garantit que l'application à vérifier n'a pas été modifiée (colonne 5, lignes 1-2) assurant de cette manière **l'intégrité** de l'application.

L'objet de la revendication 1 diffère du document D1 en ce qu'en D1 le certificat exécutable n'est pas reçu une fois que l'application logicielle à vérifier s'exécute et par conséquent il ne peut pas être déterminé préalablement à l'exécution de l'application logicielle à vérifier.

La solution proposée dans la revendication 1 de la présente demande n'est pas considérée comme inventive (article 33(3) PCT) pour les raisons suivantes :
Le document D1 décrit une méthode où des instructions critiques sont encastrées dans le code d'une application s'exécutant sur un terminal hôte connecté à une carte à puce (figure 5).

L'homme du métier reconnaîtrait que ces instructions critiques ne sont pas protégées et la nécessité de les sécuriser, de manière que le problème que se propose de résoudre la présente invention peut donc être considéré comme étant celui de sécuriser les parties critiques d'un logiciel protégé.

L'homme de du métier chercherait dans le domaine de la sécurité informatique une solution au problème et trouverait le document D2 qui décrit une "Java card" (carte à puce) séparée d'un terminal hôte qui contient les instructions de contrôle les plus critiques d'une application logicielle s'exécutant sur le terminal hôte; ces instructions de contrôle critiques étant nécessaires au correct déroulement de l'application et qui sont récupérées par le terminal hôte (page 9, ligne 21 - page 10, ligne 3).

En outre cette solution serait convenable dû au fait que D1 comprend aussi une carte à puce. L'homme de l'art serait donc incité à incorporer la solution proposée en D2 dans le procédé décrit en D1.

En conséquence l'objet de la revendication 1 n'implique pas d'activité inventive (article 33(3) PCT).

2.2 Le même argument s'applique mutatis mutandis à l'objet de la revendication indépendante correspondante 13 qui n'est donc pas non plus inventif.

3. Les revendications dépendantes 2-12 et 14-21 ne contiennent aucune caractéristique qui, en combinaison avec celles de l'une quelconque des revendications à laquelle elles se réfèrent, définisse un objet qui satisfasse aux exigences du PCT en ce qui concerne l'activité inventive, voir documents D1, D2 et D3 et les passages correspondants cités dans le rapport de recherche.

REVENDICATIONS

1. Procédé de vérification de l'intégrité d'une application logicielle exécutable dans un terminal hôte, ***caractérisé en ce qu'***il comprend les étapes suivantes :
i) déterminer au moins une suite d'instructions de contrôle formant certificat exécutable (4,15) pour l'application logicielle, exécutable par ledit terminal hôte au cours de l'exécution de l'application logicielle à vérifier (1,11),
ii) sur le terminal hôte, exécuter l'application logicielle à vérifier (1,11), recevoir le certificat exécutable (4,15) ainsi déterminé lors de l'étape i), et exécuter la suite d'instructions de contrôle dudit certificat exécutable dans le contexte mémoire dudit terminal hôte,
iii) comparer le résultat ainsi obtenu par l'exécution des instructions de contrôle avec le résultat attendu d'une application logicielle authentique et,
iv) en cas de comparaison positive, continuer le cours de l'exécution de l'application logicielle à vérifier (1,11).

2. Procédé selon la revendication 1, dans lequel le terminal hôte est équipé d'un processeur ***caractérisé en ce que*** la suite d'instructions de contrôle formant certificat (4, 15) est codée en langage interprétable par ledit processeur du terminal hôte.

3. Procédé selon la revendication 1, dans lequel le terminal hôte est équipé d'une machine virtuelle apte à émuler un processeur, ***caractérisé en ce que*** la suite d'instructions de contrôle formant certificat (4, 15) est codée en langage interprétable par la machine virtuelle du terminal hôte.

4. Procédé selon l'une des revendications 1 à 3, dans lequel le certificat exécutable comporte une partie des traitements nécessaire au bon fonctionnement de l'application authentique.

5. Procédé selon l'une des revendications 1 à 4, ***caractérisé en ce que*** dans l'étape i) il est prévu d'établir, dans un environnement sécurisé, une carte du contexte mémoire de l'application logicielle authentique en cours d'exécution, et de déterminer, à partir des valeurs de cette carte mémoire, la suite d'instructions de contrôle destinée à former le certificat exécutable (4,15).

6. Procédé selon l'une des revendications 1 à 5, ***caractérisé en ce que*** dans l'étape ii), le certificat exécutable (4, 15) à destination du terminal hôte émane d'un circuit électronique

de traitement physiquement séparé du terminal hôte.

7. Procédé selon l'une des revendications 1 à 6, ***caractérisé en ce que*** dans l'étape ii) la récupération des valeurs du contexte mémoire d'exécution se fait par lecture des valeurs aux adresses des différentes zones de la mémoire du terminal hôte, ces zones contenant les instructions exécutables et les données intrinsèques à l'application à vérifier.

8. Procédé selon l'une des revendications 1 à 7, ***caractérisé en ce que*** dans l'étape iii), le résultat obtenu par l'exécution de ladite suite d'instructions de contrôle (4,15) produit une signature de l'application à vérifier, cette signature étant calculée par ladite suite d'instructions de contrôle (4, 15) qui utilise les valeurs du contexte mémoire de l'application logicielle à vérifier en cours d'exécution de l'application.

9. Procédé selon l'une des revendications précédentes, ***caractérisé en ce que*** l'application logicielle comprend des instructions permettant de charger et d'exécuter dans sa carte de contexte mémoire ladite suite d'instructions de contrôle (4, 15) en substituant au moins une adresse d'exécution d'une instruction de ladite application logicielle par au moins une adresse d'instruction de la suite d'instructions formant certificat.

10. Procédé selon l'une des revendications précédentes, ***caractérisé en ce que*** la suite d'instructions de contrôle (4, 15) est choisie de telle sorte que l'état du contexte mémoire d'une l'application logicielle après l'exécution de la suite d'instructions de contrôle est identique et/ou sans modification de l'état du contexte mémoire de l'application logicielle avant l'exécution de la suite d'instructions de contrôle.

11. Procédé selon l'une quelconque des revendications 1 à 10, ***caractérisé en ce que*** la suite d'instructions formant certificat (4,15) est transportée dans un flux de données nécessaire à l'exécution de l'application logicielle à vérifier.

12. Procédé selon l'une quelconque des revendications 1 à 11, ***caractérisé en ce que*** l'application logicielle à vérifier est tout ou partie chiffrée, le déchiffrement correct de l'application logicielle étant réalise en cas d'intégrité de l'application logicielle à vérifier.

13. Dispositif de vérification de l'intégrité d'une application logicielle destinée à être exécutée dans un terminal hôte pour la mise en œuvre du procédé selon l'une des revendications 1 à 12, ***caractérisé en ce qu'***il comprend
- des moyens de traitement aptes à déterminer au moins une suite d'instructions de contrôle

(4,15) pour l'application logicielle (1,11), exécutable par ledit terminal hôte au cours de l'exécution de l'application logicielle, et formant un certificat exécutable de ladite application logicielle,
- des moyens d'acheminement dudit certificat exécutable jusqu'au terminal hôte et des moyens d'exécution pour exécuter la suite d'instructions formant certificat (4,15) sur ledit terminal hôte au cours de l'exécution de ladite application logicielle,
- des moyens de comparaison pour comparer le résultat obtenu par l'exécution des instructions de contrôle avec le résultat attendu d'une application authentique, et
- des moyens aptes en cas de comparaison positive à continuer l'exécution de l'application logicielle à vérifier (1,11).

14. Dispositif selon la revendication 13, ***caractérisé en ce qu***'il comprend une carte à puce ou tout autre circuit sécurisé apte à contenir la suite d'instructions de contrôle formant certificat (4,15), en ce que le terminal hôte est équipé d'un lecteur de carte à puce ou d'un moyen de communication avec le circuit sécurisé et en ce que les moyens d'exécution de l'application logicielle sont agencés pour aller chercher, dans la carte à puce ou le circuit sécurisé, la suite d'instructions formant certificat au cours de l'exécution de l'application logicielle à vérifier.

15. Dispositif selon la revendication 14, ***caractérisé en ce que*** le terminal hôte est apte à renvoyer à la carte à puce ou au circuit sécurisé la signature produite par la suite d'instructions de contrôle, et en ce que la carte à puce ou le circuit sécurisé comprend en outre une application logicielle de vérification apte à valider ou invalider l'authenticité de l'application logicielle à vérifier en fonction du résultat de la comparaison entre la signature produite par la suite d'instructions de contrôle et une valeur de la signature connue et préalablement stockée dans la carte à puce ou dans le circuit sécurisé.

16. Dispositif selon la revendication 15, ***caractérisé en ce qu***'en cas de comparaison négative, la carte à puce est apte à modifier le fonctionnement de l'application logicielle à vérifier.

17. Dispositif selon la revendication 15 ou la revendication 16, ***caractérisé en ce qu***'en cas de non transmission de la signature conformément à des conditions prédéterminées, la carte à puce est apte à modifier le fonctionnement de l'application logicielle à vérifier.

18. Dispositif selon l'une des revendications 13 à 17, ***caractérisé en ce qu***'en cas de

comparaison négative, le dispositif comprend en outre des moyens aptes à empêcher le fonctionnement de l'application logicielle dans le terminal hôte.

19. Dispositif selon l'une des revendications 13 à 18, ***caractérisé en ce que*** le terminal hôte appartient au groupe formé par les dispositifs de traitement des données, les décodeurs de télévision numérique, les équipements de visualisation de contenus multimédias, les micro-ordinateurs, les cartes à puces, les assistants personnels, les consoles de jeux, les téléphones mobiles ou analogues.

20. Dispositif selon l'une des revendications 13 à 19, ***caractérisé en ce que*** les moyens de traitement sont aptes à déterminer une pluralité de certificats exécutables (4, 15), différents les un par rapport aux autres selon une cadence et/ou condition choisie.

21. Dispositif selon l'une des revendications 13 à 20, ***caractérisé en ce que*** les moyens de traitement sont aptes à déterminer une pluralité de certificats exécutables (14, 15), différents les uns par rapport aux autres selon une cadence et/ou une condition choisie.

22. Procédé selon l'une des revendications 1 à 6, ***caractérisé en ce qu'***il comprend en outre après l'étape i), une étape consistant à insérer le certificat exécutable (4) dans un premier flot de données et à traiter par chiffrement un deuxième flot des données nécessaires au bon fonctionnement de l'application logicielle (1,11) à vérifier, avant que ledit deuxième flot ne soit accédé pour traitement par l'application logicielle (1,11) à vérifier.

23. Dispositif selon l'une des revendications 13 à 18, ***caractérisé en ce qu'***il comprend en outre des moyens aptes à insérer le certificat exécutable (4) dans un premier flot de données et des moyens de traitement par chiffrement d'un deuxième flot des données nécessaires au bon fonctionnement de l'application logicielle (1,11) à vérifier, avant que ledit deuxième flot ne soit accédé pour traitement par l'application logicielle (1,11) à vérifier.

Translation

Rec'd PCT/PTO 17 JUN 2005

PCT/FR2003/003877

PATENT COOPERATION TREATY

PCT 10/539566

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 031212	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FR2003/003877	International filing date (*day/month/year*) 23 décembre 2003 (23.12.2003)	Priority date (*day/month/year*) 24 décembre 2002 (24.12.2002)
International Patent Classification (IPC) or national classification and IPC G06F 1/00		
Applicant ENIGMA SYSTEMS SARL		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 4 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 26 juillet 2004 (26.07.2004)	Date of completion of this report 04 March 2005 (04.03.2005)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

Form PCT/IPEA/409 (cover sheet) (July 1998)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

ational application No.
PCT/FR2003/003877

I. Basis of the report

1. With regard to the **elements** of the international application:*

☐ the international application as originally filed

☒ the description:

pages 1-8, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☒ the claims:

pages _____, as originally filed
pages _____, as amended (together with any statement under Article 19
pages _____, filed with the demand
pages 1-23, filed with the letter of 03 December 2004 (03.12.2004)

☒ the drawings:

pages 1/2-2/2, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the sequence listing part of the description:

pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____

☐ the claims, Nos. _____

☐ the drawings, sheets/fig _____

5. ☒ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR 03/03877

I. Basis of the report

1. This report has been drawn on the basis of *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.)*:

Continuation of: Box I.5

Claims 22 and 23, submitted with the letter dated 3 December 2004, cause the subject matter of the application to be extended beyond the content of the application as filed. As a result, said amendments are contrary to the provisions of PCT Article 34(2)(b). The reasons are as follows:

The method in claim 22 describes two data flows, one flow that inserts the executable certificate and another flow that includes the data necessary for the software application to operate properly. However, the description (page 7, lines 6-15) mentions only one data flow that contains the control instructions (executable certificate) programmed so as to decrypt part of the data **flow** which the application to be verified must process.

The same argument applies to claim 23.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR 03/03877

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-21	YES
	Claims		NO
Inventive step (IS)	Claims		YES
	Claims	1-21	NO
Industrial applicability (IA)	Claims	1-21	YES
	Claims		NO

2. Citations and explanations

1. Reference is made to the following documents:

D1: US-B-6 308 270 1 (GUTHERY SCOTT B) 23 October 2001 (2001-10-23);

D2: WO 99/35582 A (LUI CHEW WAH) 15 July 1999 (1999-07-15);

D3: US-A-6 006 328 (DRAKE CHRISTOPHER NATHAN) 21 December 1999 (1999-12-21).

2. The present application does not fulfil the requirements set forth in PCT Article 33(1) because the subject matter of claims 1 and 13 does not involve an inventive step as defined in PCT Article 33(3), for the following reasons:

2.1 Document D1, which is considered to be the prior art closest to the subject matter of claim 1, describes (the references between parentheses apply to said document):

a method for verifying the integrity of a software application executable in a host

terminal, which method includes the following steps of:

- executing, on said host terminal, the software application to be verified and executing a series of control instructions, constituting a certificate executable by said host terminal, during the execution of the software application to be verified (column 4, line 54 to column 5, line 3; figure 5) in the memory context of said software application (column 4, line 54 to column 5, line 3);
- comparing the result from the execution of the control instructions with the result expected from an authentic software application (column 4, lines 63-65); and
- in the event of "positive comparison", continuing the execution of the software application to be verified (column 4, line 66 to column 5, line 3).

It should be noted that, in D1, the executable certificate consists of both instructions from the application to be verified that interact with a smart card, and instructions produced by said smart card. It follows that part of the executable certificate **is executed in the memory context of the software application.** It should also be pointed out that the certificate in D1 guarantees that the application to be verified has not been modified (column 5, lines 1-2) and, in this way, ensures **the integrity** of the application.

The subject matter of claim 1 differs from document D1 in that, in D1, the executable certificate is not received when the software application to be

verified is being executed and said certificate cannot, therefore, be defined prior to execution of the software application to be verified.

The solution proposed in claim 1 of the present application is not considered to be inventive (PCT Article 33(3)), for the following reasons:

Document D1 describes a method in which critical instructions are inserted into the code of an application that is being executed on a host terminal connected to a smart card (figure 5).

A person skilled in the art would recognise that said critical instructions are not protected and would acknowledge the need to secure same. As a result, the problem that the present invention is intended to solve can be considered to be that of securing the critical parts of a protected software application.

A person skilled in the art would look to the field of computer security for a solution to this problem and would find document D2, which describes a "Java card" (smart card) that is separate from a host terminal and contains the most critical control instructions for a software application being executed on the host terminal. Said critical control instructions are necessary for the application to operate properly and are retrieved by the host terminal (page 9, line 21 to page 10, line 3).

Moreover, this solution would be suitable because D1 also includes a smart card. As a result, a person

skilled in the art would be prompted to incorporate the solution proposed in D2 into the method described in D1.

It follows that the subject matter of claim 1 does not involve an inventive step (PCT Article 33(3)).

2.2 The same argument applies *mutatis mutandis* to the subject matter of the corresponding independent claim 13, which is consequently not inventive either.

3. Dependent claims 2-12 and 14-21 do not contain any features which, in combination with the features of any one of the claims to which they refer, might define subject matter that fulfils the PCT requirement of inventive step (see documents D1, D2 and D3 and the corresponding passages cited in the search report).